

ACCESS CONTROL FOR RENTAL CARS

ABSTRACT OF THE DISCLOSURE

Cars of a car rental system are made operable by having a renter present a digital key issued from the car rental system. The digital key specifies the starting date and time of a given rental transaction, and the identification of the car the key is for. The digital key is further signed by the car rental system for authenticity. A prospective renter makes online reservation over the Web and downloads into a portable storage device a digital key which can be used to operate the reserved car on the day the reservation is made for. On the pickup day, the renter goes to the car and inserts the portable storage device into a slot on the car. Upon successful verification of the digital key, the car is enabled and the renter can keep the car until he or she wants to return the car. The return process starts by having the renter obtain an invalidated digital key from the car. Once the rental car invalidates the digital key provided by the renter, the renter can no longer operate the rental car. Since the in-car controller is able to decipher the given authorization information, there is no need to re-program the in-car controller for each renter. The renter will be held liable for the rental car until he or she presents the invalidated digital key to the central station of the car rental system. To prevent a lost digital key from being used by unauthorized parties, a digital key can contain information such as a personal identification number (PIN) or a hash of the PIN of the authorized renter. For extra protection, the renter can opt to include his or her PIN in the digital key when the key is created by the car rental system. The parking lot of the car rental system can be operated without security personnel checking for proper authorization.